Beyond Security and Privacy Perception: An Approach to Biometric Authentication Perception Change

Emergent Research Forum Paper

Obi Ogbanufe
University of North Texas
Obiageli.ogbanufe@unt.edu

Dan J. Kim
University of North Texas
Dan.kim@unt.edu

Abstract

The aim of the paper is to shed light on the factors affecting perception shifts in biometrics authentication. This study explores trust relationships in the adoption of biometrics using the valence framework to understand and explain the individual's evaluation of risk concerning biometrics. Hypotheses are developed to suggest that individuals' intention to use biometrics is influenced by trust in the vendor. An experiment to test the hypotheses is described. Expected contributions, limitations, and possibilities for future research are noted.

Keywords

Biometrics, perceived security, perceived privacy, valence framework, trust.

Introduction

Over the last four decades, biometrics authentication has been extensively discussed in information systems and security literature. Some discussions raise questions about its maturity in offering the level of authenticated security required by industry, others claim that recent developments in biometrics have led to security enhancements (Havenetidis 2013) than traditional authentication methods such as username and passwords.

A biometric is the automated use of unique human physiological or behavioral characteristics to determine or verify a person's unique identity (Kleist 2007). Though not new, there is undoubted increase in the awareness and application of biometric fingerprint technology on smartphones. Coupled with payment systems like PayPal seeking to integrate with the smartphone's biometrics authentication to allow faster authentication for online payments, it is estimated that 250 million mobile devices with fingerprint biometrics will be sold in 2014. A common concern for biometrics is that its data could easily be hacked, or used for purposes other than its original intent. These concerns and recent biometrics applications illustrate the motivation for this study. Two questions are addressed. First, do individuals change their perceptions of security, privacy and convenience after the use of fingerprint biometrics for online purchase, if so how? Second, what factors influence the changes in individuals' perception?

Literature Review

Studies that examine the factors that affect the adoption and acceptance of biometrics authentication are few. Others are largely descriptive, lacking a theoretical background. Byun et al (2013), James et al (2006), and Lancelot Miltgen et al (2013) suggest that adoption of biometrics authentication is based on factors such as perceived usefulness (PU), and perceived ease of use (PEOU), risks and benefits. Wells et al. (2010) also studied the effect of novelty on the adoption of biometric hand-scanner technology and found that novelty influences adoption. However, trust – the mechanism through which individuals are able to quell concerns of security and privacy has either been omitted or not been closely examined in these studies.

Viewed as a key risk and major determinant of adoption (James, Pirim et al. 2006, Ngugi, Kamis et al. 2011), security is also seen as a value proposition for biometric authentication's positive evaluation. The storage of biometric data raises considerable security concerns for users. Kleist (2007) attempts to dispel this concern by presenting a model for managing online transactions using biometrics, and suggests that enhanced biometrics security can lead to the breakdown of trust barriers. As biometric storage solutions expand to include cloud based biometrics authentication systems, sometimes known as biometrics authentication as a service, so do questions surrounding the security of such systems. Thus, this calls for the gap in theoretically grounded literature that explores and understands security in biometrics to be filled.

The possibility that an individual's biometrics information could be used for purposes other than its original intent raises another valid concern. Privacy concerns are heightened especially when the subject matter relates to healthcare, and government surveillance (Cohn 2007). For example in healthcare, there is still apprehension that medical knowledge gained through biometrics data could be used against individuals by employers or health insurance companies. van der Ploeg (2003) describes biometric privacy issues as an emergent polemic, where one side pronounces biometrics as a malicious way to identify, track and profile individuals, and others argue that biometrics provide a solution to privacy by its ability to verify identity without disclosing name, address, or other personal data. Biometrics, not unlike other technology (e.g. location based services) is double-edged, on the one hand, individuals benefit from reduced cognitive effort and increased security, while on the other, giving up a level of privacy.

Very few biometrics studies have attempted to determine the impact of trust on risk and benefit perception. Trust has been shown to be a critical antecedent to customer acceptance in online transactions (Gefen 2000, Pavlou and Gefen 2004, Pavlou and Gefen 2005) and may be more so in the adoption of biometrics authentication in online transactions. Kleist (2007) notes that biometric technologies is poised to replicate the richness of human trust to a greater degree than other, more derivative security technologies (Kleist 2007). Despite its importance, few biometrics literature discuss trust as a determinant for biometric adoption.

Theoretical Foundation

The valence framework provides the theoretical foundation for understanding how individuals evaluate and change their perceptions of the risks and benefits of using fingerprint biometrics for online purchase. In an attempt to explain the dichotomy that exists between the positive determinants for intention to use biometrics in the form of PU and PEOU, and the negative determinants in the form of perceived security concern (PSC) and perceived privacy concern (PPC) we extend the valence perspective by integrating it with privacy calculus and perception transfer theory.

Valence Framework

Valence is defined as the degree of positive or negative feeling toward a certain option. Literature on valence framework (Peter and Tarpey 1975) posits that perceived risk and perceived benefit are two fundamental aspects of consumer decision making. On the positive and perceived benefits angle, consumers are motivated to maximize the positive aspect, while the negative and perceived risk angle presupposes that consumers are motivated to minimize the negative aspects. Using the valence framework provides the explanation that individuals will evaluate both risks and benefits before a decision is made.

There are numerous studies on the concept and impact of perceived risk, where it is defined as the probability for loss in the pursuit of an outcome (Featherman and Pavlou 2003) and as an individual's expectation of an unwanted outcome during or after an online transaction (Glover and Benbasat 2010). This study considers perceived risk of transaction in the form of (1) privacy risks, reflecting potential situations where personal and financial information are misused by the vendor; and (2) security risks, reflecting ineffective adherence to security requirements, hacking and alteration.

Biometric authentication for online transactions possesses several benefits that can be categorized as pre and post transaction benefits. Pre-transaction benefits are benefits individuals experience prior to a purchase, such as reduced cognitive effort and ease of use. For example, individuals experience the benefit

of reduced cognitive effort when there is no need to remember the correct username/password for each transaction. Post transaction benefits include nonrepudiation of transactions, fraud reduction, faster transaction, and usefulness. For example, individuals experience reliable authentication knowing their biometric trait is unique, and not easily replicated. Together, the pre and post transaction benefits constitute perceived benefits of payment method using biometrics authentication.

Privacy Calculus Theory

The calculus theory of information privacy sees a users' privacy as give and take where users disclose their personal information in exchange for expected benefits. Information privacy refers to the ability of the individual to control the terms under which personal information is acquired and used (Westin, 1967). It has been shown that the calculus perspective of privacy is the most useful framework for analyzing consumer privacy concerns (Culnan and Bies 2003). Value is provided to individuals in terms of faster, more secure access to products and services, in exchange for personal information. In this study, we use the valence framework as the overarching theory and the privacy calculus to explain the negative valence evaluation.

Perception Transfer Theory

The perception transfer theory posits that individuals' perceptions towards an object are transferred from perceptions of other reference objects associated with the target object (Stewart 2003, 2006). For example, in the case of this study, an individual with an already established trust of online vendor may transfer this trust to the security and privacy of the biometric authentication. This study tests the transfer of trust from the biometrics provider to the perception the user has about security and privacy. Sun et al (2014) in their study of web to mobile service transition used perception transfer theory to explain the moderating effect of trust between operational consistency and intention. In this study, we attempt to explain the impact trust plays in moderating perceptions of risks to the user.

Research Model and Hypotheses

The research model (Figure 1) provides a representation of both the benefits and the risks associated with using biometrics authentication. We suggest that trust of the vendor moderates both the effects of PPC and PSC, and the effects of PU and PEOU. The technology acceptance model (TAM) (Davis 1989) is used in this study to explain important determinants - PU and PEOU - of individuals' continued intention to use.

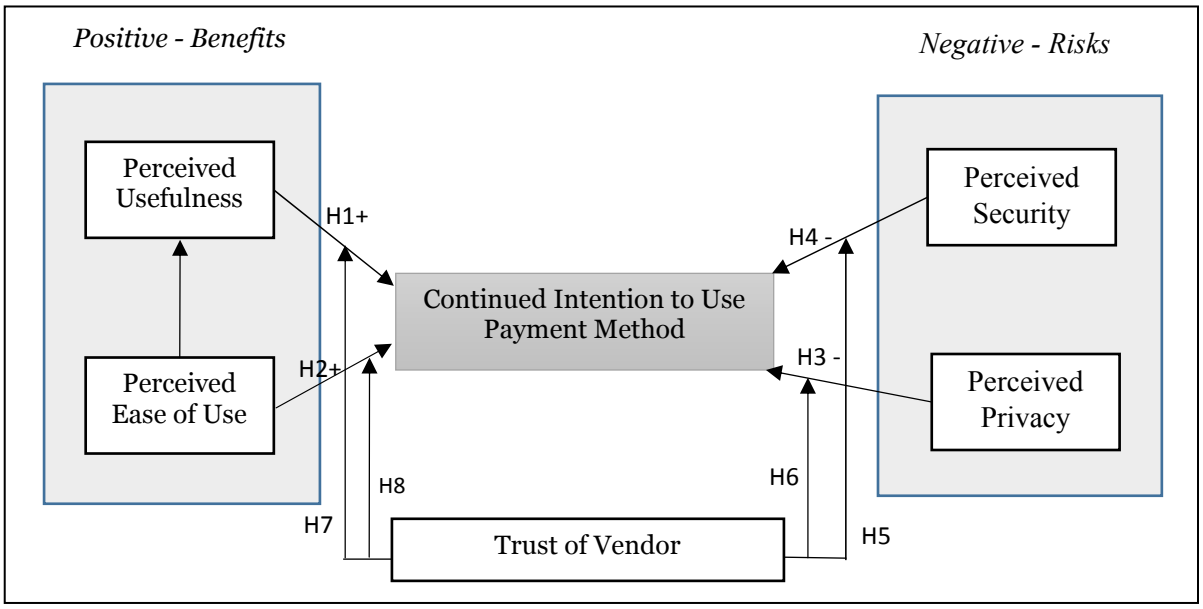

Figure 1: Research Model

Perceived Benefits of Biometrics Authentication

Using valence framework as a backdrop for the evaluation of positive versus negative options, we propose perceived benefits of biometrics authentication as the positive effects of using biometrics technology. The anticipation of usefulness, ease of use, and reduced cognitive effort provide the basis for the benefits users may experience, which positively influences intention to use biometrics authentication. Consistent with prior research on technology adoption, PU reflects the users' anticipation that using the systems will increase their performance, and PEOU reflects the users' expectation that the target system is free from effort (Davis, Bagozzi et al. 1989). Therefore, we hypothesize:

H1: PU is positively associated with intention to continue to use payment method

H2: PEOU is positively associated with intention to continue to use payment method

Perceived Risks of Biometrics Authentication

Perceived risk is viewed as the negative side, and the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm (Malhotra, Kim et al. 2004). PPC is the degree to which a consumer believes that s/he has lost control over the collection and use of their personal information (Xu, Dinev et al. 2011), and PSC is the degree to which a consumer feels unprotected against security threats resulting from the use (Jain et al. 2004). The anticipation of risk in the form of PSC and PPC is expected to have a negative influence on intention. Concerns for security of personal information seem reasonable given the nature of the data, and the effect to the individual if breached. While traditional authentication methods (e.g. username/password) can be changed when compromised, biometrics data consists of irrevocability, i.e. if compromised it becomes impossible to issue the individual with a replacement fingerprint (Whitley, Gal et al. 2014). Therefore we posit that:

H3: PPC is negatively associated with continued intention to use biometrics payment method.

H4: PSC is negatively associated with continued intention to use biometrics payment method.

Moderating Role of Trust

Perceived security has been found to be a key predictor in influencing consumers' intention to transact online. As a result of the nature of the acquisition and measurement of biometric data, perceived security concerns are anticipated to be heightened. In this situation, trust of the vendor and payment instrument becomes more important, necessitating an even more complex belief requirement that the vendor makes effort to fulfill commitments, and does not seek to take unfair advantage of the consumer (Quiqley et al 2007, McKnight et al 2002). Trust of Vendor (TOV) is defined as the degree to which consumers are willing to be vulnerable to another party (Mayer and Davis 1999). Trust alleviates perceptions of risks (Mayer et al 1995), and serves to moderate the individual's perception of security risks inherent in biometrics authentication. Moorman et al. (1992) note that trust reduces "perceived uncertainty and hence the perceived vulnerability" (p. 315), thus meaning that trusting beliefs are expected to mitigate risk perceptions (Malhotra, Kim et al. 2004). We posit that individuals who express greater trust in the vendor will exhibit lower perceptions of security risk than individuals who do not trust the vendor.

H5. The effect of PSC on intention to continue to use payment method will be moderated by TOV such that this effect will be weaker (stronger) when TOV is high (low)

H6. The effect of PPC on intention to continue to use payment method will be moderated by TOV such that this effect will be weaker (stronger) when TOV is high (low)

Using perception transfer theory, when individuals' trust in vendor is very high, and without consideration for the PU and PEOU of biometric authentication, the relationship between PU/PEOU and intention to use biometrics authentication will be relatively weak. For instance when an individual owner

of the iPhone has developed a high level of trust of Apple – represented here as the vendor – the individual pays less attention to usefulness and ease of use of the biometrics as a determinant of its use, because the individual may have already formed a trust of Apple. Fang et al (2014) noted that when perceptions of institutional mechanism is high, in our case represented as trust in the vendor, the less additional assurance is needed for increasing the individual's confidence towards the intended behavior. Thus we theorize that a TOV negatively moderates the relationship between PU and intention; and similarly, TOV negatively moderates the relationship between PEOU and intention.

H7: The effect of PU on Intention to continue to use payment method is moderated by TOV such that it is weakened (strengthened) when trust of vendor is high (low).

H8: The effect of PEOU on Intention to continue to use payment method is moderated by TOV such that it is weakened (strengthened) when trust of vendor is high (low).

Methodology

We will examine the proposed research model and hypotheses using an experiment. We will develop a simple simulated website for song purchase. To differentiate the levels of convenience, security, and privacy, we will implement two types of login process (i.e., username/password login and biometric fingerprint login) and three payment methods on the website. Considering these two types of login processes and three payment methods, we will develop treatment combinations. Since username/password login and simple credit card payment method is a typical transaction method, it will be used as a baseline for the comparison of other treatment combinations. Subjects will go through an orientation that provides an explanation of the study and procedures. After orientation, subjects will be assigned a task of shopping for songs, and randomly assigned to each treatment. All instruments are completed online.

Expected Results

The study expects to show that as individuals seek more secure ways to authenticate using biometrics, trust will be a major factor, and that trust will attenuate the perceptions of privacy and security concerns. Furthermore, it expects to explain the individual's evaluation of biometrics risks, how trust moderates the relationships between risks and intention. This study's contribution is in the validation of the valence framework, privacy calculus and perception transfer theory in explaining risk evaluations and the transfer of trust in spite of risks.

Common with experiments is the limitation of external validity. Since individuals are not actually expending their income on the purchase, the effect of trust on risks and benefits may be reduced.

As biometric authentication technology expands into social media and the cloud, it becomes even more important to understand how trust and risks influence biometrics perceptions, and use intentions. The intersection of biometrics, cloud and social media represents a promising space for future IS research and practice.

REFERENCES

Byun, S., & Byun, S.-E. (2013). Exploring perceptions toward biometric technology in service encounters: a comparison of current users and potential adopters. Behaviour & Information Technology, 32(3), 217-230. doi: 10.1080/0144929X.2011.553741

Cohn, M. (2007). Biometrics: Key to securing consumer trust. Biometric Technology Today, 15(3), 8-9. doi: http://dx.doi.org/10.1016/S0969-4765(07)70082-6

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues, 59(2), 323-342. doi: 10.1111/1540-4560.00067

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology (Vol. 13).

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of two Theoretical Models (Vol. 35).

Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," International journal of human-computer studies (59:4), pp. 451-474.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. Omega, 28(6), 725-737.

Glover, S., and Benbasat, I. 2010. "A Comprehensive Model of Perceived Risk of E-Commerce Transactions," International Journal of Electronic Commerce (15:2), pp. 47-78.

Havenetidis, K. (2013). Encryption and Biometrics: Context, methodologies and perspectives of biological data. Journal of Applied Mathematics and Bioinformatics, 3(4), 141-161.

Jain, A. K., Ross, A., and Prabhakar, S. 2004. "An Introduction to Biometric Recognition," Circuits and Systems for Video Technology, IEEE Transactions on (14:1), pp. 4-20.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. Journal of Organizational and End User Computing, 18(3), 1-24.

Kleist, V. F. P. (2007). Building Technologically Based Online Trust: Can the Biometrics Industry Deliver the Online Trust Silver Bullet? Information Systems Management, 24(4), 319-329.

Lancelot Miltgen, C., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. Decision Support Systems, 56(0), 103-114. doi: http://dx.doi.org/10.1016/j.dss.2013.05.010

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," Information Systems Research (15:4), pp. 336-355.

Mayer, R. C., and Davis, J. H. 1999. "The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-Experiment," Journal of applied psychology (84:1), p. 123.

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," Academy of management review (20:3), pp. 709-734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: an integrative typology. Information Systems Research, 13(3), 334-359.

Moorman, C., Zaltman, G., & Deshpande, R. (1992). Relationships between Providers and Users of Market Research: The Dynamics of Trust Within and Between Organizations. Journal of Marketing Research (JMR), 29(3), 314-328.

Ngugi, B., Kahn, B. K., & Tremaine, M. (2011). Typing Biometrics: Impact of Human Learning on Performance Quality. J. Data and Information Quality, 2(2), 1-21. doi: 10.1145/1891879.1891884

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. Information Systems Research, 15(1), 37-59.

Pavlou, P. A., and Gefen, D. 2005. "Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role," Information Systems Research (16:4), pp. 372-399.

Peter, J. P., & Tarpey Sr, L. X. (1975). A comparative analysis of three consumer decision strategies. Journal of Consumer Research, 29-37.

Quigley, N. R., Tesluk, P. E., Locke, E. A., and Bartol, K. M. 2007. "A Multilevel Investigation of the Motivational Mechanisms Underlying Knowledge Sharing and Performance," Organization Science (18:1), pp. 71-88.

Stewart, K. J. (2003). Trust transfer on the World Wide Web. Organization Science, 14(1), 5-17.

Sun, Y., Shen, X.-L., and Wang, N. 2014. "Understanding the Role of Consistency During Web–Mobile Service Transition: Dimensions and Boundary Conditions," International Journal of Information Management (34:4), pp. 465-473.

van der Ploeg, I. (2003). Biometrics and Privacy A note on the politics of theorizing technology. Information, Communication & Society, 6(1), 85-104. doi: 10.1080/1369118032000068741

Venkatesh, V., Morris, M. G., Gordon, B. D., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425-478. doi: 10.2307/30036540

Wells, J. D., Campbell, D. E., Valacich, J. S., & Featherman, M. (2010). The Effect of Perceived Novelty on the Adoption of Information Technology Innovations: A Risk/Reward Perspective. Decision Sciences, 41(4), 813-843. doi: 10.1111/j.1540-5915.2010.00292.x

Whitley, E. A., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. European Journal of Information Systems, 23(1), 17-35.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: linking individual perceptions with institutional privacy assurances. Paper presented at the Journal of the Association for Information Systems.

Westin, A.F. Privacy and Freedom. New York: Atheneum, 1967